Notice of Allowability	Application No.	Applicant(s)	
	10/769,104	SANDU ET AL.	
	Examiner	Art Unit	
	TESHOME HAILU	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/02/2009*.

2. ☒ The allowed claim(s) is/are *1, 4-5, 7-9, 12, 14-16, 18-20 and 23*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12/17/2009* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. In an amendment filed on November 02, 2009, claims 1, 4-5, 7-9, 12, 14-16 and 18-20 have been amended.

2. Claims 2-3, 6, 10-11, 13, 17 and 21-22 have been cancelled.

3. Claim 23 has been added.

4. Claims 1, 4-5, 7-9, 12, 14-16, 18-20 and 23 are pending.

Response to Arguments

5. Applicant's arguments filed on September 15, 2008, with respect to the rejection of claims 1, 4-5, 7-9, 12, 14-16 and 18-20 have been fully considered in view of the remarks and amendment to claims and are persuasive. The rejections of claims 1, 4-5, 7-9, 12, 14-16 and 18-20 have been withdrawn.

Claim Objections

6. Claim is objected to because of the following informalities: The comparison module of the claim 1 is repeatedly claimed in paragraph 4 and 6 of claim 1. Applicant authorized the examiner to amend this claim in the examiner amendment.

Allowable Subject Matter

7. Claims 1, 4-5, 7-9, 12, 14-16, 18-20 and 23 are allowed. No reason for allowance is needed as the record is clear in light of applicant's arguments and specification.

EXAMINER'S AMENDMENT

8. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant representative, Jens C. Jenkins (Reg. No. 44,803), on December 17, 2009. The following amendment to claim 1 will replace the previous claim 1.

1. (Currently Amended) A computer-implemented malware detection system for determining whether an executable script is malware according to ~~its functionality,~~ functional variables and subroutines of the executable script, the malware detection system comprising:

a malware signature store including at least one known malware script signature, wherein each malware signature in the malware signature store is a normalized signature of a known malware script; [[and]]

a normalization module that obtains an executable script and generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises normalizing ~~tokens~~ variables and subroutines from the executable script into normalized ~~tokens~~ variables and subroutines conforming to a common format suitable for comparison with that at least one malware signature in the malware signature store, the normalizing comprising renaming variables and subroutines from the executable script according to a common naming convention; and

a comparison module, wherein the comparison module compares the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store;

wherein the malware detection system is configured to:

~~compare the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store to determine whether the executable script is malware; and report whether the executable script is malware according to the determination, comprising~~ determining determine whether the comparison found a complete match between the normalized signature for the executable script and the at least one normalize malware signature, and if so, reporting that the executable script is malware.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Teshome Hailu/

Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434